RELATED INTERPRETATIONS OF ELLIPTIC CURVES

ALEKSANDER SKENDERI

Abstract. The goal of this expository paper is to explore the relations between many interpretations of elliptic curves over $\mathbb{C}$. Introducing elliptic curves as algebraic varieties, we then discuss their algebraic interpretation as groups, their topological interpretation as complex tori, and briefly also mention the complex analytic structures that they possess. Thus the study of elliptic curves serves as a beautiful representation of the unity of mathematics, using tools from algebra, topology, and analysis. This paper assumes a good familiarity with fundamental ideas in algebra, complex analysis, and hyperbolic geometry.

Contents

1. Introduction 1
2. The Group Law on Elliptic Curves 2
2.1. Preliminaries on Algebraic Plane Curves 2
2.2. Lattices and Fundamental Regions 2
2.3. Basic Results on Elliptic Functions 4
2.4. An Addition Theorem and the Group Law 9
3. Complex Tori and Elliptic Curves 11
3.1. Tori and Moduli 12
3.2. The Modular Function 13
3.3. The Lattice Associated to a Cubic 15
Acknowledgments 20
References 20

1. Introduction

The study of elliptic curves is interesting for many reasons. One such reason is the incredible role they play in modern mathematics, such as in the proofs of the Modularity Theorem and Fermat's Last Theorem. Another reason, that which concerns this paper, is that the study of elliptic curves serves to relate many different branches of mathematics; indeed, algebra, analysis, and topology all play a role in the study of elliptic curves. The goal of this paper is to precisely elucidate these relations. Beginning with the definition of an elliptic curve as the zero set of a particular polynomial, we then discuss how elliptic curves can be thought of as groups and complex tori, and briefly also discuss the analytic structures they possess.

2. The Group Law on Elliptic Curves

2.1. **Preliminaries on Algebraic Plane Curves.** Let k be a field of characteristic different from 2 or 3, and define the *affine plane* $\mathbb{A}_k^2$ to be the set of all points (a, b) with $a, b \in k$. An *affine plane curve* is the collection of all points (x, y) in $\mathbb{A}_k^2$ that satisfy

$$f(x, y) = 0, \tag{2.1}$$

for some nonconstant polynomial $f \in k[x, y]$. Typically, the field k we will be working with will be either $\mathbb{R}$ or $\mathbb{C}$. The degree of the polynomial f in (2.1) is also called the *degree of the curve*. A degree 2 curve is called a *conic* and a degree 3 curve is called a *cubic*. In the Euclidean space $\mathbb{R}^2$, the familiar examples of conics are the parabola, ellipse, and hyperbola. We will be primarily interested in cubics; in particular, in a special type of cubic called an *elliptic curve*. We first need the following definition.

Definition 2.2. A point P is a *singular point* or *singularity* of the affine curve defined by $f(x, y) = 0$ if

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

A point is *nonsingular* if it is not singular, and a curve all of whose points are nonsingular is called *nonsingular* or *smooth*.

Definition 2.3. An *elliptic curve* is the set of points defined by an equation of the form

$$y^2 = x^3 + ax + b,$$

where the cubic $f(x, y) = y^2 - x^3 - ax - b$ is nonsingular.

A priori it is not intuitively clear that one can impose a group law on such a curve. Our present goal is to show how this is possible.

2.2. **Lattices and Fundamental Regions.** Let f be a function defined on the complex plane $\mathbb{C}$. A complex number $\omega \in \mathbb{C}$ is called a *period of* f if

$$f(z + \omega) = f(z)$$

for all $z \in \mathbb{C}$. The function f is called *periodic* if it has a period $\omega \neq 0$. Familiar examples of periodic functions are $\sin z$ and $\cos z$, which have a period 2π, and the exponential function e^z, which has a period $2\pi i$. The set of periods of each of these functions is of the form $\Omega = \{n\omega : n \in \mathbb{Z}\}$, for some fixed $\omega \in \mathbb{C} \setminus \{0\}$, and is therefore isomorphic to the integers $\mathbb{Z}$. The functions we are presently interested in will have their set of periods of the form

$$\Omega(\omega_1, \omega_2) = \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\},$$

for some fixed $\omega_1, \omega_2 \in \mathbb{C} \setminus \{0\}$, where ω_1 and ω_2 are linearly independent over $\mathbb{R}$; such a set is called a *lattice*. Notice that $\Omega(\omega_1, \omega_2) \cong \mathbb{Z} \times \mathbb{Z}$. If f contains some lattice in its set of periods, then f is said to be *doubly periodic*. Currently, our only example of doubly periodic functions are the constant functions. It is a nontrivial task to construct nonconstant doubly periodic functions, as we shall soon see. We first discuss a few more properties of lattices. If $\Omega(\omega_1, \omega_2)$ has the set $\{\omega_1, \omega_2\}$

as a basis, it is clear that it can have many other types of bases. For instance, $\{\omega_1 + \omega_2, \omega_2\}$ is also a basis, since if $\omega \in \Omega(\omega_1, \omega_2)$, then

$$\omega = n\omega_1 + m\omega_2 = n(\omega_1 + \omega_2) + (m - n)\omega_2,$$

where $n, m - n \in \mathbb{Z}$. The following simple exercise in linear algebra explains how we find other bases in more generality.

Lemma 2.4. *Let a, b, c, and d be integers and let $\Omega(\omega_1, \omega_2)$ be a lattice. The equations*

$$\omega_2' = a\omega_2 + b\omega_1$$
$$\omega_1' = c\omega_2 + d\omega_1$$

define a basis for $\Omega(\omega_1, \omega_2)$ if and only if $ad - bc = \pm 1$.

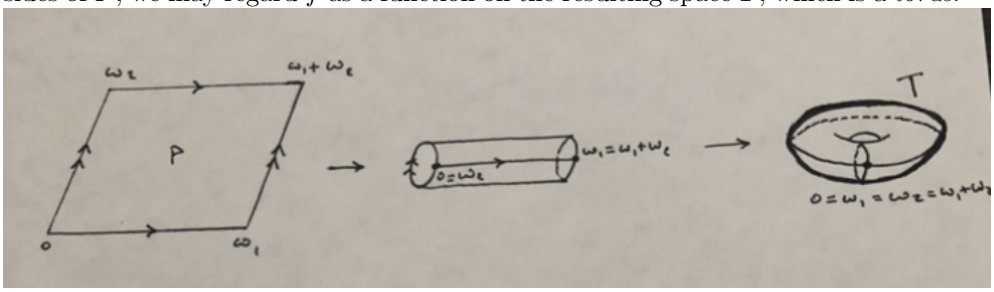
Proof. See section 3.4 of [1]. □

Given a lattice Ω, we say that $z_1, z_2 \in \mathbb{C}$ are *congruent* mod Ω, written $z_1 \sim z_2$ mod Ω (or simply $z_1 \sim z_2$) if $z_1 - z_2 \in \Omega$. This is easily seen to be an equivalence relation, with the equivalence classes being the cosets $z + \Omega$ of the subgroup Ω of the additive group $\mathbb{C}$. Since each $\omega \in \Omega$ induces the translation $t_\omega : z \mapsto z + \omega$ of $\mathbb{C}$, and since $t_{\omega_1+\omega_2} = t_{\omega_1} \circ t_{\omega_2}$ we have a group isomorphism $\Omega \cong \{t_\omega : \omega \in \Omega\}$. Hence, two points of $\mathbb{C}$ are congruent mod Ω if and only if they lie in the same orbit under the action of Ω on $\mathbb{C}$.

Definition 2.5. A closed, connected subset P of $\mathbb{C}$ is said to be a *fundamental region* for Ω if

(i) for each $z \in \mathbb{C}$, P contains at least one point in the same Ω-orbit as z, and
(ii) no two points in the interior of P are in the same Ω-orbit.

We will mostly be interested in the case when P is a parallelogram, in which case it is called a *fundamental parallelogram*. The key point in this definition is that a fundamental region P provides a *tesellation* of the plane $\mathbb{C}$ under the action of Ω; that is, the translates $P + \omega = \{z + \omega : z \in P\}$, $\omega \in \Omega$, cover all of $\mathbb{C}$, and overlap only at their boundaries. Thus, if f is doubly periodic with respect to a lattice $\Omega = \Omega(\omega_1, \omega_2)$, we can determine its behavior on $\mathbb{C}$ by analyzing its behavior on any fundamental region P; this is analogous to how the behavior of a simply periodic function, such as $\sin z$, is determined by its behavior on an interval. Let P be a fundamental parallelogram with verticies 0, ω_1, ω_2, and $\omega_1 + \omega_2$. By definition, f takes the same values on congruent boundary points, and so by identifying the opposite sides of P, we may regard f as a function on the resulting space T, which is a *torus*.



By the definition of a fundamental region, we have a bijection between the set of points on the torus and the orbits of Ω on $\mathbb{C}$. Hence, we can think of T as the set

of Ω-orbits on $\mathbb{C}$; that is T is the collection of cosets $\mathbb{C}/\Omega$. Since $\mathbb{C}$ is abelian, the subgroup Ω is normal, and thus $T = \mathbb{C}/\Omega$ has the structure of an abelian group. Furthermore, T is compact since the function that identifies boundary points is a continuous function from the compact set P onto T.

2.3. **Basic Results on Elliptic Functions.**

Definition 2.6. A meromorphic function $f : \mathbb{C} \to \Sigma := \mathbb{C} \cup \{\infty\}$ is *elliptic* with respect to a lattice $\Omega \subset \mathbb{C}$ if f is doubly periodic with respect to Ω. [1]

If f is elliptic with respect to Ω, then our previous discussion shows that we may regard f as a function $f : T \to \Sigma$, where T is the torus $T = \mathbb{C}/\Omega$. Fix $c \in \Sigma$ and suppose f is not identically equal to c. As f is meromorphic, the solutions of $f(z) = c$ must be isolated, and each solution must have finite multiplicity, with congruent solutions $z_1, z_2 \in \mathbb{C}$ having the same multiplicity (i.e., they are zeroes of the same order for the function $g(z) = f(z) - c$). If P is a fundamental parallelogram for Ω, then the compactness of P and the fact that the solutions of $f(z) = c$ are isolated shows that P contains only finitely many of these solutions. By replacing P by $P + w$ ($w \in \mathbb{C}$) if necessary, we can assume that there are no solutions on the boundary ∂P of P. Let the solutions within P be $z = z_1, ..., z_n$, with multiplicities $k_1, ..., k_n$. Set $N = k_1 + ... + k_n$. Then there are N solutions, counting multiplicities, of $f(z) = c$ within P. As $z_1, ..., z_n$ are representatives for the congruence classes of solutions of $f(z) = c$ for $z \in \mathbb{C}$, we may view N as the sum of the multiplicities of the solutions of $f([z]) = c$, where $[z] \in T = \mathbb{C}/\Omega$ is the congruence class corresponding to $z \in \mathbb{C}$. This leads to the following definition.

Definition 2.7. The *order* $\mathrm{ord}(f)$ of an elliptic function $f : \mathbb{C}/\Omega \to \Sigma$ is the number of solutions, counting multiplicites, of $f([z]) = \infty$; that is, it is the sum of the orders of the congruence classes of the poles of f.

For the following theorems, we assume that f is elliptic with respect to $\Omega = \Omega(\omega_1, \omega_2)$, that $\mathrm{ord}(f) = N$, and that P is a fundamental parallelogram for Ω having verticies $t, t + \omega_1, t + \omega_2, t + \omega_1 + \omega_2$, where $t \in \mathbb{C}$ is chosen so that ∂P contains no zeroes or poles of f.

Theorem 2.8. *The function f is constant if and only if $N = 0$ (in particular, any analytic elliptic function must be constant).*

Proof. If f is constant, then it is analytic. Hence it has no poles in $\mathbb{C}$, and thus $N = 0$. Conversely, suppose that $N = 0$, so that f has no poles in $\mathbb{C}$, and is therefore analytic. By the definition of P, we have $f(P) = f(\mathbb{C})$. As P is compact and f is continuous, $f(P) \subset \mathbb{C}$ is compact, and therefore bounded. Hence f is a bounded, entire function on $\mathbb{C}$, whence Liouville's theorem implies that f must be constant. □

Theorem 2.9. *The sum of the residues of f within P is zero.*

Proof. Since f is meromorphic and ∂P was chosen so as not to contain any zeroes or poles of f, we see that the sum of the residues of f within P is given by $\frac{1}{2\pi i} \int_{\partial P} f(z)dz$. Let $\Gamma_1, \Gamma_2, \Gamma_3$, and Γ_4 be the sides of P connecting t and $t + \omega_1$,

[1] For a historical perspective on elliptic functions, see section 3.6 of [1].

$t+\omega_1$ and $t+\omega_1+\omega_2$, $t+\omega_1+\omega_2$ and $t+\omega_2$, and t, respectively, so that the orientation of ∂P is the counterclockwise (positive) orientation. Then,

$$\frac{1}{2\pi i}\int_{\partial P} f(z)dz = \frac{1}{2\pi i}\sum_{k=1}^{4}\int_{\Gamma_k} f(z)dz. \tag{2.10}$$

Now as ω_2 is a period of f and $\Gamma_3 = \Gamma_1 + \omega_2$ with the reverse orientation, we obtain

$$\int_{\Gamma_1} f(z)dz = \int_{\Gamma_1} f(z+\omega_2)dz = -\int_{\Gamma_3} f(z+\omega_2)d(z+\omega_2) = -\int_{\Gamma_3} f(z)dz,$$

where in the last equality, with an abuse of notation, we performed a change of variables setting $z-\omega_2$ for z. A similar argument shows that $\int_{\Gamma_2} f(z)dz = -\int_{\Gamma_4} f(z)dz$. By (2.10), we see that the sum of the residues of f within P is zero. □

Corollary 2.11. *There are no elliptic functions of order $N = 1$.*

Proof. If f were an elliptic function of order $N = 1$, then f would have a single residue of order 1 at some point $z_0 \in P$. In some small neighborhood of z_0, the function f then has a Laurent series expansion

$$f(z) = \sum_{n=-1}^{\infty} a_n(z-z_0)^n,$$

where $a_{-1} \neq 0$. Then the sum of the resides of f within P is $a_{-1} \neq 0$, contradicting the preceding theorem. □

Theorem 2.12. *If f has order $N > 0$, then f takes each value $c \in \Sigma$ exactly N times.*

Proof. If $c = \infty$, then this is just the definition of N; assume then that $c \in \mathbb{C}$. Replacing f by $f - c$ (which has the same order as f), we may assume that $c = 0$. Now f'/f is meromorphic and ∂P contains no zeroes or poles of f, so that f'/f is analytic on ∂P. Furthermore, since f is elliptic, so is f', and thus so is the quotient f'/f . Thus integrating f'/f around ∂P and applying the argument of Theorem 2.9, we see that

$$\int_{\partial P} \frac{f'(z)}{f(z)}dz = 0.$$

By Cauchy's Argument Principle, we conclude that f has the same number of zeroes as its number of poles, counting multiplicities. Thus, $f(z) = 0$ has exactly N solutions, as desired. □

Corollary 2.11 tells us that if we want nonconstant elliptic functions, then they must have order at least 2. Just as how the familiar trigonometric and exponential functions are obtained by means of power series, elliptic functions will be obtained by means of power series; the only difference now is that the indexing set is some lattice $\Omega = \Omega(\omega_1, \omega_2)$. As the series we consider are typically absolutely convergent, they are invariant under rearrangements, and so the particular order of the series is not essential. It is not too difficult to construct elliptic functions of order $N \geq 3$, as the following theorem shows.

Theorem 2.13. *For each integer $N \geq 3$, the function $F_N(z) = \sum_{\omega\in\Omega}(z-\omega)^{-N}$ is elliptic of order N with respect to Ω.*

Proof. See Theorem 3.9.3 of [1]. □

The proof is primarily based upon the fact for $s \in \mathbb{R}$, the series $\sum_{\omega \in \Omega \setminus \{0\}} |\omega|^{-s}$ converges if and only if $s > 2$ (notice the similarity with how the series $\sum_{n \in \mathbb{N} \setminus \{0\}} |n|^{-s}$ converges if and only if $s > 1$). Thus, in order to obtain elliptic functions of order 2, we need to subtract an additional term from the summand to guarantee absolute convergence.

Definition 2.14. The *Weierstrass $\wp$ function* associated to a lattice Ω, denoted by $\wp(z, \Omega)$ (or just $\wp(z)$, when the lattice is understood) is defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{2.15}$$

We now show that this represents an elliptic function of order 2. One shows that this series represents a well-defined meromorphic function by comparing it with the series $\sum_{\omega \in \Omega \setminus \{0\}} |\omega|^{-3}$ in a similar fashion to the argument of Theorem 2.13. In particular, this argument shows that it is uniformly convergent on compact subsets of $\mathbb{C}$, so that we can differentiate and integrate this series term-by-term. A more interesting question is how one shows that it is elliptic. Indeed, this is not clear a priori, as the series is not of the form $\sum_{\omega \in \Omega} f(z - \omega)$. Our method is based upon relating $\wp$ to one of the series $F_N(z)$ mentioned above.

Theorem 2.16. *The function $\wp(z)$ is an elliptic function with Ω as its lattice $\Omega_\wp$ of periods.*

Proof. We described above how to show that $\wp(z)$ is meromorphic, so we only show that $\Omega = \Omega_\wp$. As the series (2.15) defining $\wp(z)$ is uniformly convergent on compact subsets of $\mathbb{C}$, we can differentiate term-by-term to obtain

$$\wp'(z) = \frac{-2}{z^3} - \sum_{\omega \in \Omega \setminus \{0\}} \left(\frac{2}{(z-\omega)^3} \right) = -2 \sum_{\omega \in \Omega} \frac{1}{(z-\omega)^3} = -2F_3(z),$$

where $F_3(z)$ is elliptic of order 3 by Theorem 2.13. We conclude that for each $\omega \in \Omega$, $\wp'(z+\omega) - \wp'(z) = 0$, so that $\wp(z+w) - \wp(z)$ is some constant c_ω. Setting $z = -\omega/2$ and noticing that $\wp(z)$ is even, we find that

$$c_\omega = \wp\Big(\frac{\omega}{2}\Big) - \wp\Big(-\frac{\omega}{2}\Big) = 0,$$

showing that each $\omega \in \Omega$ is a period of $\wp(z)$. Thus, $\Omega \subset \Omega_\wp$. To prove the reverse inclusion, we notice that since 0 is a pole of $\wp(z)$, there is a pole of $\wp(z)$ at every point in $\Omega_\wp$. But the expression for $\wp(z)$ shows that it has no poles in $\mathbb{C} \setminus \Omega$. Hence, $\Omega_\wp \subset \Omega$. □

Theorem 2.17. *$\wp(z)$ has order 2 and $\wp'(z)$ has order 3.*

Proof. $\wp(z)$ has a pole of order 2 at each lattice point and no other poles. Thus it has a single congruence class of poles of order 2, showing that it has order 2. In the above proof, we saw that $\wp'(z) = -2F_3(z)$. Since $F_3(z)$ has a single congruence class of poles of order 3, $\wp'(z)$ has order 3. □

It is a theorem that the field of all even elliptic functions over $\mathbb{C}$ is precisely the field of rational functions in $\wp(z)$, and that the field of all elliptic functions over $\mathbb{C}$ is the field of rational functions in $\wp(z)$ and $\wp'(z)$ (see Theorem 3.11.1 of

[1]). Thus, just as every simply periodic meromorphic function has a Fourier series expansion in terms of $\sin(z)$ and $\cos(z)$ (with even functions being expressed solely in terms of $\cos(z)$), where $\sin(z)$ and $\cos(z)$ are related by $\sin'(z) = \cos(z)$, we have similar results for elliptic functions. We also know that $\sin(z)$ and $\cos(z)$ satisfy the algebraic equation $x^2 + y^2 - 1 = 0$, where $x = \cos(z)$ and $y = \sin(z)$. It is then natural to ask whether $\wp(z)$ and $\wp'(z)$ satisfy a similar equation. Moreover, since the algebraic equation relating $\sin(z)$ and $\cos(z)$ is what gives us parametrizations of conics such as the circle and (more generally) the ellipse, we should be hopeful that if we find an algebraic equation connecting $\wp(z)$ and $\wp'(z)$, then we might be able to parametrize some type of plane curve. We now derive the differential equation relating $\wp(z)$ and $\wp'(z)$, and then explain how this allows us to induce the group law on an elliptic curve.

To derive this equation, we need to find a Laurent series for $\wp(z)$ in a small neighborhood of $z = 0$. We begin by obtaining a Laurent series for the function

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \in \Omega \setminus \{0\}} \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right). \tag{2.18}$$

Let $m = \min\{|\omega| : \omega \in \Omega \setminus \{0\}\}$, and let $D = \{z \in \mathbb{C} : |z| < m\}$ be the largest open disc centered at zero containing no nonzero lattice point of Ω. Since

$$\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2} = \frac{z^2}{\omega^2(z - \omega)},$$

we see by comparison with $\sum_{\omega \in \Omega \setminus \{0\}} |\omega|^{-3}$ that $\zeta(z)$ is absolutely convergent for all $z \in \mathbb{C} \setminus \Omega$ (and uniformly convergent on compact subsets of $\mathbb{C}$ where this series is defined, so that it may be differentiated term-by-term). Additionally, for all $\omega \in \Omega \setminus \{0\}$, the binomial series

$$\frac{1}{z - \omega} = -\sum_{n=1}^{\infty} \frac{z^{n-1}}{\omega^n}$$

is absolutely convergent for all $z \in D$. We may then substitute this expression in (2.18) to obtain the Laurent series

$$\begin{aligned} \zeta(z) &= \frac{1}{z} + \sum_{\omega \in \Omega \setminus \{0\}} \left(-\frac{z^2}{\omega^3} - \frac{z^3}{\omega^4} - \ldots \right) \\ &= \frac{1}{z} - \sum_{n=2}^{\infty} G_{n+1} z^n, \end{aligned}$$

valid for all $z \in D$, where

$$G_k = G_k(\Omega) = \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-k}.$$

The G_k give what is called the *Eisenstein series* for Ω. Notice that they are absolutely convergent for all $k \geq 3$ by Theorem 2.13. For odd k, we have that $(-\omega)^k = -\omega^k$, yielding $G_k = 0$. The Laurent series for $\zeta(z)$ then simplifies to

$$\zeta(z) = \frac{1}{z} - \sum_{n=2}^{\infty} G_{2n} z^{2n-1},$$

for $z \in D$. Differentiating, we find that

$$\wp(z) = -\zeta'(z) = \frac{1}{z^2} + \sum_{n=2}^{\infty} (2n-1)G_{2n} z^{2n-2},$$

yielding a Laurent series for $\wp(z)$, valid for $z \in D$. By explicitly writing out the first several terms for the power series $\wp'(z)^2, 4\wp(z)^3$, and $60G_4\wp(z)$, we find that

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = z^2\phi(z), \tag{2.19}$$

where $\phi(z)$ is some power series convergent in D. Since $\wp$ and $\wp'$ are elliptic with respect to Ω, so is the left hand side of (2.19), which we denote by $f(z)$. Now $f(z) = z^2\phi(z)$ in D, and since $f(0) = 0$, this implies that f vanishes at all $\omega \in \Omega$. But by construction, f can only have poles at the poles of $\wp$ or $\wp'$, which are the lattice points of Ω. Hence f is analytic, and so by Theorem 2.8 f must be constant; this constant is 0 as $f(0) = 0$. This proves that

Theorem 2.20. $\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$.

It is traditional to write $g_2(\Omega) = g_2$ for $60G_4$ and $g_3(\Omega) = g_3$ for $140G_6$ so that this differential equation becomes

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3. \tag{2.21}$$

This suggests that we may be able to parametrize the elliptic curve $y^2 = 4x^3 - g_2x - g_3$ by setting $x = \wp(z)$ and $y = \wp'(z)$. To show that we can indeed do this, we need the following results.

Theorem 2.22. *Let Ω be a lattice with basis $\{\omega_1, \omega_2\}$, and let $\omega_3 = \omega_1 + \omega_2$. If P is a fundamental parallelogram for Ω having $0, \frac{1}{2}\omega_1, \frac{1}{2}\omega_2$, and $\frac{1}{2}\omega_3$ in its interior, then $\frac{1}{2}\omega_1, \frac{1}{2}\omega_2$, and $\frac{1}{2}\omega_3$ are the zeroes of $\wp'$ in P.*

Proof. By Theorem 2.17, we know that $\wp'(z)$ has three poles and three zeroes in P, counting multiplicity. Since $\wp'(z)$ is odd, if $\omega \in \Omega$ satisfies $\frac{1}{2}\omega \sim -\frac{1}{2}\omega \bmod \Omega$, then $\wp'(\frac{1}{2}\omega) = -\wp'(\frac{1}{2}\omega)$, so that $\wp'(\frac{1}{2}\omega)$ is either 0 or ∞. Since $\wp'$ has a pole of order 3 at $0 \in P$, we conclude that $\frac{1}{2}\omega_1, \frac{1}{2}\omega_2$, and $\frac{1}{2}\omega_3$ are the zeroes of $\wp'$ in P. □

We now define $e_j := \wp(\frac{1}{2}\omega_j)$ for $j = 1, 2, 3$. As $S = [\frac{1}{2}\omega_1] \cup [\frac{1}{2}\omega_2] \cup [\frac{1}{2}\omega_3]$ is the set of all zeroes of $\wp'$ in $\mathbb{C}$, we deduce that $\{e_1, e_2, e_3\} = \wp(S)$ is independent of the particular choice of basis $\{\omega_1, \omega_2\}$ of Ω.

Corollary 2.23. *For all $c \in \Sigma \setminus \{e_1, e_2, e_3\}$, the equation $\wp(z) = c$ has two simple solutions; for $c = e_1, e_2, e_3$, or ∞, the equation has one double solution.*

Proof. By Theorems 2.12 and 2.17, $\wp(z)$ takes each value $c \in \Sigma$ twice, giving either two simple solutions (z and $-z$, since $\wp(z)$ is even) or one double solution. If $c \in \mathbb{C}$, then $\wp(z) = c$ has a double solution if and only if $\wp'(z) = 0$, so that $z \sim \frac{1}{2}\omega_j \bmod \Omega$ (where $j = 1, 2, 3$), showing that $c = e_j$. If $c = \infty$, then $\wp(z)$ has a double pole at $z = 0$, and so $\wp(z) = \infty$ has a double solution. □

Theorem 2.24. *The values e_1, e_2, and e_3 are mutually distinct.*

Proof. Consider $f_j(z) = \wp(z) - e_j$ for $j = 1, 2, 3$. Since the poles of the f_j are the same as those of $\wp(z)$, the f_j are elliptic functions of order 2 and therefore each has two classes of zeroes, counting multiplicities. Since

$$f_j\Big(\frac{1}{2}\omega_j\Big) = f_j'\Big(\frac{1}{2}\omega_j\Big) = 0,$$

f_j has a double class of zeroes on $[\frac{1}{2}\omega_j]$ and thus no other zeroes. This implies that $f_j(\frac{1}{2}\omega_k) \neq 0$ for $j \neq k$; that is, $e_j \neq e_k$ for $j \neq k$. □

By the differential equation (2.21), we see that the polynomial $p(x) = 4x^3 - g_2x - g_3$ has its zeroes at the points $x = \wp(z)$ where $\wp'(z) = 0$. Thus, the above results show that $p(x)$ has the three distinct zeroes e_1, e_2, and e_3.

2.4. **An Addition Theorem and the Group Law.** From the differential equation $(\wp'(z))^2 = p(\wp(z))$, where $p(x) = 4x^3 - g_2x - g_3$, we see that each $t \in \mathbb{C}/\Omega$ determines a point $(\wp(t), \wp'(t))$ on the elliptic curve

$$E = \{(x, y) \in \Sigma \times \Sigma : y^2 = p(x)\}.$$

As we now show, the converse is also true. Moreover, the parametrization of E in terms of $\wp$ and $\wp'$ shows that E is topologically equivalent (over $\mathbb{C}$, in the analytic topology) to the torus $\mathbb{C}/\Omega$. [2]

Theorem 2.25. *The map $\theta : \mathbb{C}/\Omega \to E$ given by $\theta(t) = (\wp(t), \wp'(t))$ is a homeomorphism.*

Proof. By Corollary 2.23, we know that $t_0 = [0]$ is the only point mapped to (∞, ∞) and that $t_j = [\frac{1}{2}\omega_j]$ are the only points mapped to $(e_j, 0)$, where $j = 1, 2, 3$, respectively. If $(x, y) \in E$ is any other point, then $x \neq \infty, e_j$ and $y \neq \infty, 0$. Corollary 2.23 then tells us that the equation $\wp(t) = x$ has two simple solutions $t = \pm t_1$. As $\wp'$ is odd, we have that $\wp'(t_1) = -\wp'(-t_1) \neq \wp'(-t_1)$ (as $t_1 \neq [\frac{1}{2}\omega_j]$). Hence, one of either $\wp'(t_1)$ or $\wp'(-t_1)$ takes the value of $y = \sqrt{p(x)} = \sqrt{p(\wp(t))}$, so that one of $\pm t_1$ is mapped uniquely onto (x, y) by θ. This shows that θ is a bijection. Finally, as $\wp$ and $\wp'$ are meromorphic and nonconstant, they are continuous open maps; hence so is θ, showing that both θ and θ^{-1} are continuous. □

We saw earlier that $T = \mathbb{C}/\Omega$ has the structure of an abelian group. If $P_1 = \theta(t_1)$ and $P_2 = \theta(t_2)$ are any two points in E, then we can impose an abelian group structure on E by simply defining $P_1 + P_2 = \theta(t_1 + t_2)$. The above theorem showed that θ was a bjiection, so that we have forced θ to be an isomorphism. Using this, we see that the identity element on E is

$$\theta([0]) = (\wp(0), \wp'(0)) = (\infty, \infty).$$

If $\theta(t) = (x, y) \in E$, then its inverse is

$$\theta(-t) = (\wp(-t), \wp'(-t)) = (\wp(t), -\wp'(t)) = (x, -y).$$

If our elliptic curve E were a subset of $\mathbb{R}^2 \cup \{(\infty, \infty)\}$ instead of $\Sigma \times \Sigma$, then finding the inverse of $(x, y) \in E \setminus \{(\infty, \infty)\}$ amounts to reflecting the point about the x-axis.

Describing the sum of two points on an elliptic curve in terms of their coordinates is more difficult. Let $P_j = \theta(t_j)$, $j = 1, 2$, be two points on E. Then

$$P_1 + P_2 = \theta(t_1 + t_2) = (\wp(t_1 + t_2), \wp'(t_1 + t_2)).$$

So as to avoid trivial cases, we assume P_1, P_2, and $P_1 + P_2$ are all non-zero in E. If we can find an addition theorem for the Weierstrass $\wp$ function, then we can also express the coordinates of $P_1 + P_2$ in terms of those of P_1 and P_2. Recall that a

[2]Notice that we have defined E as a subset of $\Sigma \times \Sigma \cong \mathbb{P}^1 \times \mathbb{P}^1$, instead of as a subset of $\mathbb{P}^2$, as it is typically defined. However, in both cases E is the one-point compactification of the finite part of the elliptic curve, and so the two perspectives can in this way be seen as the same.

function f is said to possess an *addition theorem* if there exists a non-zero rational function R with complex coefficients in three variables satisfying

$$R(f(z_1), f(z_2), f(z_1 + z_2)) = 0$$

for all $z_1, z_2 \in \mathbb{C}$ (familiar examples of functions possessing addition theorems include the exponential and trigonometric functions). As we already have a differential equation relating $\wp$ and $\wp'$, it would be very useful if we could construct an elliptic function g in terms of $\wp$ and $\wp'$ that also possesses some relation between t_1, t_2, and $t_1 + t_2$. For this we need the following theorem, whose proof follows a similar strategy to that of Theorem 2.12, and is therefore omitted; the interested reader may consult Theorem 3.6.7 in [1].

Theorem 2.26. *Let f be an elliptic function with respect to a lattice Ω having congruence classes of zeroes and poles $[a_1], ..., [a_r]$ and $[b_1], ..., [b_s]$, with multiplicities $k_1, ..., k_r$, and $l_1, ..., l_s$, respectively. Then,*

$$\sum_{j=1}^{r} k_j a_j \sim \sum_{j=1}^{s} l_j b_j \bmod \Omega.$$

By this theorem, if we can construct an elliptic function g of order 3 having a triple pole at $[0]$ and simple zeroes at t_1 and t_2 (or a double zero at t_1, if $t_1 = t_2$), then the third zero t_3 of g must satisfy $t_1 + t_2 + t_3 = [0]$. That is, $t_3 = -(t_1 + t_2)$, and so $P_1 + P_2 = \theta(-t_3) = (\wp(t_3), -\wp'(t_3))$. We now construct such a function g. Consider the function

$$g(t) = \wp'(t) - \alpha\wp(t) - \beta, \tag{2.27}$$

where $\alpha, \beta \in \mathbb{C}$ are to be determined. Then g is certainly elliptic of order 3, and has a triple pole at $[0]$. If $t_1 \neq t_2$, then g has the required zeroes provided that

$$\wp'(t_j) = \alpha\wp(t_j) + \beta, \text{ that is,}$$

$$y_j = \alpha x_j + \beta. \tag{2.28}$$

where $(x_j, y_j) = (\wp(t_j), \wp'(t_j))$ for $j = 1, 2$. Since $t_1 + t_2 \neq [0]$ by hypothesis, we have $t_1 \neq \pm t_2$. We also have $t_1, t_2 \neq [0]$, and so x_1 and x_2 are distinct and finite. Thus we can find $\alpha, \beta \in \mathbb{C}$ satisfying (2.28). As $t_3 = -(t_1 + t_2)$ is also a root, $(x_3, y_3) = (\wp(t_3), \wp'(t_3))$ also satisfies (2.28). Continuing with the assumption that $t_1 \neq t_2$, (2.28) yields

$$\alpha = \frac{y_1 - y_2}{x_1 - x_2}. \tag{2.29}$$

As $y_j^2 = p(x_j)$, we have

$$p(x_j) - (\alpha x_j + \beta)^2 = 0,$$

for $j = 1, 2, 3$. That is, the x_j are the roots of the polynomial

$$4x^3 - \alpha^2 x^2 - (2\alpha\beta + g_2)x - (\beta^2 + g_3) = 0. \tag{2.30}$$

Using the formula for the sum of the roots, we obtain

$$x_1 + x_2 + x_3 = \frac{\alpha^2}{4}.$$

Now using (2.29) and that $\wp(t_1+t_2)=\wp(-(t_1+t_2))=\wp(t_3)=x_3$, we have

$$\wp(t_1+t_2)=\frac{1}{4}\left(\frac{\wp'(t_1)-\wp'(t_2)}{\wp(t_1)-\wp(t_2)}\right)^2-\wp(t_1)-\wp(t_2), \tag{2.31}$$

provided $t_1, t_2, t_1 \pm t_2 \neq [0]$. This gives us the addition theorem for $\wp$ (stricly speaking, we would have to use the relation between $(\wp')^2 = p(\wp)$ to obtain an expression solely in terms of $\wp$, but this is not essential for our purposes).

Returning to the group structure of E, we see that $P_1+P_2=(\wp(t_3),-\wp'(t_3))=(x_3,-y_3)$ has coordinates

$$x_3=\wp(t_3)=\wp(t_1+t_2)=\frac{1}{4}\left(\frac{y_1-y_2}{x_1-x_2}\right)^2-x_1-x_2,$$

and

$$y_3=\alpha x_3+\beta,$$

where

$$\beta=y_1-\alpha x_1=\frac{x_1y_2-y_1x_2}{x_1-x_2},$$

and thus

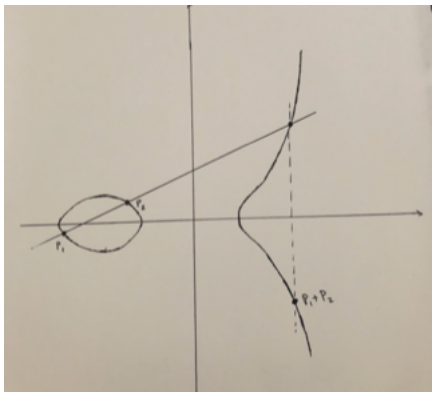
$$y_3=\frac{(x_3-x_2)y_1-(x_3-x_1)y_2}{x_1-x_2}.$$

Thus, we can express the coordinates of P_1+P_2 in terms of rational expressions of the coordinates of P_1 and P_2.

To interpret this geometrically, let

$$E_{\mathbb{R}}:=\{(x,y)\in E : x,y\in\mathbb{R}\}\cup\{(\infty,\infty)\}.$$

By the preceeding results, $E_{\mathbb{R}}$ is a subgroup of E. Now by (2.28), the points (x_j,y_j), $j=1,2,3$ are collinear. Thus the point $P_1+P_2\in E_{\mathbb{R}}$ is obtained by taking the reflection along the x-axis of the third point of intersection of $E_{\mathbb{R}}$ and the line connecting P_1 and P_2.



3. Complex Tori and Elliptic Curves

We saw earlier that given a lattice $\Omega\subset\mathbb{C}$, we can construct a homeomorphism between the complex torus $\mathbb{C}/\Omega$ and the elliptic curve E defined by $y^2=4x^3-g_2(\Omega)x-g_3(\Omega)$ by parametrizing E by means of elliptic functions on $\mathbb{C}/\Omega$. The goal of this section is to explain under what conditions the converse holds. To this end,

we will employ some basic results from hyperbolic geometry; references [1] and [6] provide excellent treatments of this subject for the uninitiated reader.

3.1. **Tori and Moduli.** One of the difficulties we face in attempting to associate a torus to an elliptic curve is that there may be many tori that are homeomorphic to a given elliptic curve. If we can impose an equivalence relation on the set of all complex tori, then we are in a better position to investigate our question. But any two complex tori $\mathbb{C}/\Omega$ and $\mathbb{C}/\Omega'$ are determined by their lattices Ω and Ω', and so it suffices to impose an equivalence relation on the set of all lattices in $\mathbb{C}$.

Definition 3.1. Two lattices $\Omega, \Omega' \subset \mathbb{C}$ are said to be *similar* or *homothetic* if there exists some $\mu \in \mathbb{C} \setminus \{0\}$ such that $\Omega' = \mu\Omega := \{\mu\omega : \omega \in \Omega\}$.

It is not difficult to check that this is an equivalence relation. Furthermore, it is a non-trivial result that two complex tori $\mathbb{C}/\Omega$ and $\mathbb{C}/\Omega'$ are conformally equivalent (meaning that they have the same complex analytic structures) if and only if Ω and Ω' are similar (see Theorem 4.18.1 of [1]). Our present goal now becomes to determine when two tori are similar; that is, we want to construct a function on the set of all complex tori that takes on the same value at different tori if and only if the tori are similar.

By Lemma 2.4, if $\{\omega_1, \omega_2\}$ and $\{\omega_1', \omega_2'\}$ are bases for Ω and $\Omega' = \mu\Omega$, where $\mu \in \mathbb{C} \setminus \{0\}$, then there exist $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$ such that

$$\begin{aligned} \omega_2' &= \mu(a\omega_2 + b\omega_1), \\ \omega_1' &= \mu(c\omega_2 + d\omega_1). \end{aligned} \tag{3.2}$$

As ω_1 and ω_2 are linearly independent over $\mathbb{R}$, we have $\text{Im}\ (\omega_2/\omega_1) \neq 0$. Interchanging ω_1 and ω_2 if necessary, we can assume that $\text{Im}\ (\omega_2/\omega_1) > 0$. We now define the *modulus* of the basis $\{\omega_1, \omega_2\}$ to be

$$\tau = \frac{\omega_2}{\omega_1},$$

where the numbering of the basis elements is chosen so that $\text{Im}(\tau) > 0$. As each lattice Ω has many bases, it determines a set of moduli. Since $\mu\omega_2/\mu\omega_1 = \omega_2/\omega_1$, similar lattices have the same set of moduli. Setting $\tau = \omega_2/\omega_1$ and $\tau' = \omega_2'/\omega_1'$ (the moduli of the above bases for Ω and Ω'), we see from (3.2) that Ω and Ω' are similar if and only if

$$\tau' = \frac{a\tau + b}{c\tau + d}, \tag{3.3}$$

where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$. By the definition of the modulus of a basis, both τ and τ' lie in the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$. Now if $ad - bc = -1$, then the Möbius transformation $T : z \mapsto (az + b)/(cz + d)$ maps $\mathbb{H}$ onto the lower half-plane, and we must therefore have $ad - bc = 1$. Conversely, if $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$, then from (3.2) we have a basis $\{\omega_1', \omega_2'\}$ for a lattice Ω' that is similar to Ω. Recall that the collection of all Möbius transformations $T : z \mapsto (az + b)/(cz + d)$ with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$ forms the discrete subgroup $\text{PSL}(2, \mathbb{Z})$ of $\text{PSL}(2, \mathbb{R})$, which is called the *modular group* and which we will denote by Γ. Our above argument has proved the following:

Theorem 3.4. *If $\Omega = \Omega(\omega_1, \omega_2)$ and $\Omega' = \Omega'(\omega_1', \omega_2')$ are lattices in $\mathbb{C}$ with moduli $\tau = \omega_2/\omega_1$ and $\tau' = \omega_2'/\omega_1'$, then Ω and Ω' are similar if and only if $\tau' = T(\tau)$ for some $T \in \Gamma$.*

In other words, we can think of the equivalence classes of similar lattices as corresponding to points of the quotient-space $\mathbb{H}/\Gamma$.

3.2. **The Modular Function.** By Theorem 3.4, we have converted our problem of determining when two lattices are similar to the problem of constructing a function that takes on the same value at two points $\tau, \tau' \in \mathbb{H}$ if and only if τ and τ' lie in the some orbit of the action of Γ on $\mathbb{H}$. Previously, we saw that the Weierstrass $\wp$ function satisfies the differential equation $\wp' = \sqrt{p(\wp)}$, where p is a cubic polynomial of the form

$$p(z) = 4z^3 - c_2 z - c_3 \quad (c_2, c_3 \in \mathbb{C}). \tag{3.5}$$

A polynomial of the form (3.5) is said to be in *Weierstrass normal form.* Since any cubic polynomial can be brought in this form by means of a substitution of the type $\phi : z \mapsto az + b$ $(a, b \in \mathbb{C}, a \neq 0)$ and since $\phi : \mathbb{C} \to \mathbb{C}$ is a bijection preserving the multiplicities of roots, we will henceforth restrict our attention to polynomials p in Weierstrass normal form. If e_1, e_2, and e_3 are the roots of our polynomial p in (3.5), then we define the *discriminant* of p to be

$$\Delta_p = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_1 - e_3)^2,$$

where we see that the e_i are distinct if and only if $\Delta_p \neq 0$.[3] Using the definition of the discriminant and the relations between the roots of a polynomial and its coefficients, it is relatively straightforward to see that $\Delta_p = c_2^3 - 27c_3^2$ (see section 6.2 of [1], for example). As an immediate consequence, we deduce the following:

Corollary 3.6. *The polynomial $p(z) = 4z^3 - c_2 z - c_3$ has distinct roots if and only if $c_2^3 - 27c_3^2 \neq 0$.*

By Theorem 2.20, we know that the Weierstrass $\wp$ function associated to the lattice Ω satisfies $\wp'(z) = \sqrt{p(\wp)}$, where $p(z) = 4z^3 - g_2 z - g_3$ and

$$g_2 = g_2(\Omega) = 60 \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-4},$$

$$g_3 = g_3(\Omega) = 140 \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-6}.$$

If we let $\Delta(\Omega)$ denote the discriminant Δ_p of p, then by Theorem 2.24 and Corollary 3.6, we see that $\Delta(\Omega) = g_2(\Omega)^3 - 27g_3(\Omega)^2 \neq 0$. Thus we may define the *modular function* $J(\Omega)$ by

$$J(\Omega) = \frac{g_2(\Omega)^3}{\Delta(\Omega)} = \frac{g_2(\Omega)^3}{g_2(\Omega)^3 - 27g_3(\Omega)^2}. \tag{3.7}$$

Now for a similar lattice $\mu\Omega$ (here $\mu \neq 0$), we have

$$g_2(\mu\Omega) = 60 \sum_{\omega \in \Omega \setminus \{0\}} (\mu\omega)^{-4} = \mu^{-4} g_2(\Omega),$$

$$g_3(\mu\Omega) = 140 \sum_{\omega \in \Omega \setminus \{0\}} (\mu\omega)^{-6} = \mu^{-6} g_3(\Omega), \text{ and}$$

$$\Delta(\mu\Omega) = \mu^{-12}\Delta(\Omega).$$

[3] This definition of the discriminant differs from how it is usually presented in texts on abstract algebra; we have included the factor of 16 to conclude that $\Delta_p = c_2^3 - 27c_3^2$.

Therefore

$$J(\mu\Omega) = J(\Omega) \tag{3.8}$$

for all $\mu \in \mathbb{C} \setminus \{0\}$, showing that similar lattices determine the same value of J.

In order to regard g_2, g_3, Δ, and J as functions on the upper half-plane $\mathbb{H}$, we evaluate them at $\tau \in \mathbb{H}$ by evaluating them on the lattice $\Omega(1, \tau)$ that has τ as one of its moduli. We then obtain

$$\begin{aligned} g_2(\tau) &= 60 \sum_{m,n\in\mathbb{Z}\setminus\{0\}} (m+n\tau)^{-4}, \text{ and} \\ g_3(\tau) &= 140 \sum_{m,n\in\mathbb{Z}\setminus\{0\}} (m+n\tau)^{-6}. \end{aligned} \tag{3.9}$$

Additionally,

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^3, \tag{3.10}$$

and

$$J(\tau) = \frac{g_2(\tau)^3}{\Delta(\tau)}.$$

Now if $\tau' = T(\tau)$ for some $T \in \Gamma$, then by Theorem 3.4 the lattices $\Omega = \Omega(1, \tau)$ and $\Omega' = \Omega'(1, \tau')$ are similar, and so (3.8) implies that $J(\Omega) = J(\Omega')$. This proves the following:

Theorem 3.11. *$J(T(\tau)) = J(\tau)$ for all $\tau \in \mathbb{H}$ and $T \in \Gamma$.*

Thus $J(\tau)$ is invariant under the action of the modular group Γ. It will also be useful to understand how the action of Γ, as well as the orientation reversing transformations of $\mathbb{H}$, affect g_2, g_3, and Δ. Firstly, if $T : \tau \mapsto (a\tau + b)/(c\tau + d)$ is an element of Γ, then

$$\begin{aligned} g_2(T(\tau)) &= 60 \sum_{m,n\in\mathbb{Z}\setminus\{0\}} \left(m + n\frac{(a\tau+b)}{(c\tau+d)}\right)^{-4} \\ &= 60(c\tau+d)^{-4} \sum_{m,n\in\mathbb{Z}\setminus\{0\}} ((md+nb) + (mc+na)\tau)^{-4}. \end{aligned}$$

Since $ad - bc = 1$, Lemma 2.4 implies that the transformation $(m, n) \mapsto (md + nb, mc + na)$ simply permutes the elements of the set $(m, n) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0, 0)\}$. Then by the absolute convergence of our series (Theorem 2.13), we can rearrange the elements to obtain

$$g_2(T(\tau)) = 60(c\tau+d)^{-4} \sum_{m,n\in\mathbb{Z}\setminus\{0\}} (m+n\tau)^{-4} = (c\tau+d)^{-4} g_2(\tau). \tag{3.12}$$

We similarly find that

$$g_3(T(\tau)) = (c\tau+d)^{-6} g_3(\tau), \tag{3.13}$$

and finally that

$$\Delta(T(\tau)) = (c\tau+d)^{-12} \Delta(\tau), \tag{3.14}$$

from which we immediately deduce another proof of Theorem 3.11. In the particular case when $a = b = d = 1$ and $c = 0$ so that $T : \tau \mapsto \tau + 1$, we have the following result:

Theorem 3.15. *The functions $g_2(\tau)$, $g_3(\tau)$, $\Delta(\tau)$, and $J(\tau)$ are periodic with respect to $\mathbb{Z}$.*

We will also need to understand how the above functions behave under the action of the orientation reversing transformations of $\mathbb{H}$, which are those of the form

$$T(\tau) = \frac{a\overline{\tau} + b}{c\overline{\tau} + d}, \quad (a, b, c, d \in \mathbb{Z}, ad - bc = -1). \tag{3.16}$$

Entirely analogous computations to those performed above show that

$$\begin{aligned} g_2(T(\tau)) &= (c\overline{\tau} + d)^{-4}\overline{g_2(\tau)}, \\ g_3(T(\tau)) &= (c\overline{\tau} + d)^{-6}\overline{g_3(\tau)}, \\ \Delta(T(\tau)) &= (c\overline{\tau} + d)^{-12}\overline{\Delta(\tau)}, \text{ and} \\ J(T(\tau)) &= \overline{J(\tau)}. \end{aligned} \tag{3.17}$$

These formulas will soon play an important role in allowing us to show that J provides us with a surjection of the upper half-plane $\mathbb{H}$ onto the complex plane $\mathbb{C}$. In particular, we will show that each $c \in \mathbb{C}$ is the pre-image under J of precisely one orbit of the action of Γ on $\mathbb{H}$. Before we can do this, we still need a bit more information about $g_2(\tau), g_3(\tau), \Delta(\tau)$, and $J(\tau)$. The proofs of the following results are not conceptually difficult, but are rather long and technical; we now state the results without proof, so as not to detract from the main idea of our current exposition. For the proofs, see section 6.4 of [1].

Theorem 3.18. *The functions g_2, g_3, Δ, and $J : \mathbb{H} \to \mathbb{C}$ are analytic on $\mathbb{H}$.*

Theorem 3.19. *Let $\tau \in \mathbb{H}$ and write $q = e^{2\pi i\tau}$ so that $0 < |q| < 1$. Then the modular function $J : \mathbb{H} \to \mathbb{C}$ has a Laurent series expansion*

$$J(\tau) = \frac{1}{1728}\left(\frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n\right),$$

where the c_n are all integers.

3.3. **The Lattice Associated to a Cubic.** In this section, we achieve our aim of proving that if $p(z) = 4z^3 - c_2 z - c_3$ is a polynomial in the Weierstrass normal form (3.5) with distinct roots, then there exists a lattice Ω such that $g_k(\Omega) = c_k$ for $k = 2, 3$. The key ingredient in this proof is the fact that J surjects $\mathbb{H}$ onto $\mathbb{C}$. To prove this statement, we first need some more basic results.

Lemma 3.20. *Let $\tau \in \mathbb{H}$.*

(i) *If $2Re(\tau) \in \mathbb{Z}$, then $g_2(\tau), g_3(\tau), \Delta(\tau)$, and $J(\tau)$ are all real.*
(ii) *If $|\tau| = 1$, then $g_2(\tau) = \tau^4\overline{g_2(\tau)}$, $g_3(\tau) = \tau^6\overline{g_3(\tau)}$, $\Delta(\tau) = \tau^{12}\overline{\Delta(\tau)}$, and $J(\tau) = \overline{J(\tau)}$.*

Proof. The main idea of both parts is to use the hypotheses on τ to construct an orientation reversing transformation of $\mathbb{H}$ that fixes τ. In this way, the equations (3.17) give us relations between the images of τ under the functions g_2, g_3, Δ, and J, and the conjugates of these images, respectively.

(*i*) If $2\ \mathrm{Re}(\tau) = n \in \mathbb{Z}$, then τ is fixed by the map $T : \tau \to n - \overline{\tau}$, which is of the form (3.16), with $a = -1, b = n, c = 0, d = 1$. The result is now immediate from (3.17).

(*ii*) If $|\tau| = 1$, then τ is fixed by the map $T : \tau \to 1/\overline{\tau}$ (geometrically, this map represents the composition of an inversion with respect to the unit circle and reflection about the real axis). This map is again of the form (3.16), now with $a = 0, b = 1, c = 1$, and $d = 0$. Thus by (3.17), we obtain

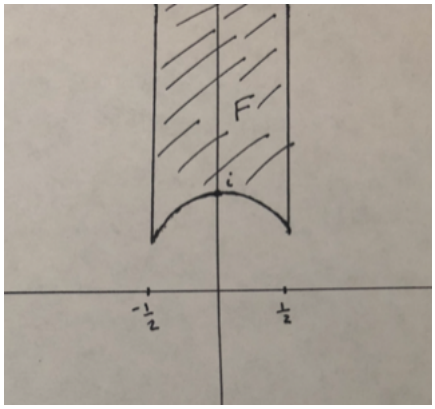
$$g_2(\tau) = g_2(1/\overline{\tau}) = (\overline{\tau})^{-4}\overline{g_2(\tau)} = \tau^4\overline{g_2(\tau)},$$

and similarly for the other functions. □

Recalling that the modular group Γ has as a fundamental region the set

$$F = \left\{\tau \in \mathbb{H} : |\tau| \geq 1 \text{ and } |\mathrm{Re}(\tau)| \ \leq \frac{1}{2}\right\},$$

the previous result allows us to immediately deduce the following.



Corollary 3.21. *$J(\tau)$ is real whenever τ is on the imaginary axis or on the boundary ∂F of F.*

Furthermore, Lemma 3.20 allows us to compute the value of J at certain special points on ∂F.

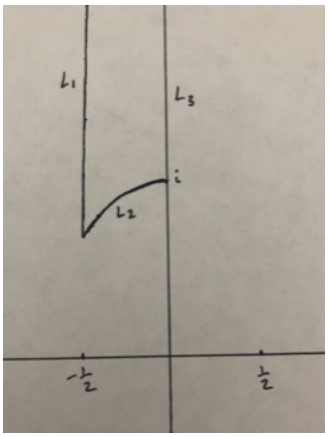
Corollary 3.22. *Let $\rho = e^{2\pi i/3}$. Then $g_2(\rho) = g_3(i) = J(\rho) = 0$ and $J(i) = 1$.*

Proof. Part (*i*) of Lemma 3.20 shows that g_2 and g_3 both take on real values at the points i and ρ. This along with part (*ii*) of the lemma shows that $g_2(\rho) = \rho g_2(\rho)$ and $g_3(i) = -g_3(i)$. Therefore, $g_2(\rho) = g_3(i) = 0$, and by the formula for J we also obtain $J(\rho) = 0$ and $J(i) = 1$. □

Now, let $L = L_1 \cup L_2 \cup L_3$ be the boundary of the portion of F contained in the second quadrant, where

$$L_1 = \left\{\tau \in \mathbb{H} : |\tau| \geq 1 \text{ and } \mathrm{Re}(\tau) = -\frac{1}{2}\right\},$$
$$L_2 = \left\{\tau \in \mathbb{H} : |\tau| = 1 \text{ and } -\frac{1}{2} \leq \mathrm{Re}(\tau) \leq 0\right\},$$
$$L_3 = \left\{\tau \in \mathbb{H} : |\tau| \geq 1 \text{ and } \mathrm{Re}(\tau) = 0\right\},$$

as illustrated below.



By Corollary 3.21, we know that $J(L) \subset \mathbb{R}$. We now show that the reverse inclusion also holds.

Theorem 3.23. *The modular function J maps the set L onto $\mathbb{R}$.*

Proof. The main idea is to use the Laurent series expansion of J given in Theorem 3.19 to deduce some topological information about the image set $J(L)$. The fact that J is analytic on $\mathbb{H}$, which is guaranteed by Theorem 3.18, will then force $J(L) = \mathbb{R}$.

If $\tau \in L_3$, then we have $\tau = iy$ for $y \geq 1$. Hence $q = e^{2\pi i\tau} = e^{-2\pi y}$, and as $y \to \infty$, we have $q \to 0$, through positive real values. Since

$$J(\tau) = \frac{1}{1728}\left(\frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n\right).$$

we have $J(\tau) \to \infty$ as $q \to 0$. Similarly if $\tau \in L_1$, then $\tau = -1/2 + iy$, where $y \geq 1$, and therefore $q = -e^{-2\pi y}$. Thus as $y \to \infty$, we have $q \to 0$ through negative real values, and therefore $J(\tau) \to -\infty$. This shows that as a real-valued function on L (Corollary 3.21), J is unbounded from above and below. But Theorem 3.18 tells us that J is analytic on $\mathbb{H}$, and so, in particular, J is continuous on $\mathbb{H}$; since L is connected, it follows that $J(L)$ is connected. But any connected subset of $\mathbb{R}$ that is unbounded from above and below must be $\mathbb{R}$ itself, and thus $J(L) = \mathbb{R}$. □

Notice that if we did not include the set L_2 in the definition of L, but simply defined $L = L_1 \cup L_3$, then the above argument would not work, since L would then not be connected.

The following result is the culmination of our studies of the J function and will play a crucial role in proving the main theorem of this section.

Theorem 3.24. *For each $c \in \mathbb{C}$, there is exactly one orbit of Γ in $\mathbb{H}$ on which J takes the value c.*

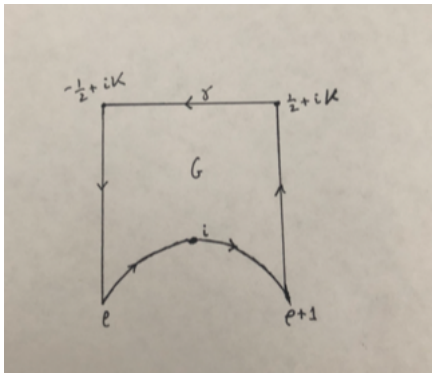
Proof. By the definition of a fundamental region for a Fuchsian group, we know that each orbit of Γ meets F at either a unique point in the interior F° of F, or at one or two equivalent points on ∂F.

Suppose first that $c \in \mathbb{C} \setminus \mathbb{R}$. By Corollary 3.21 we have $J(\partial F) \subset \mathbb{R}$ (more precisely, by using Theorem 3.23, we have $J(\partial F) = \mathbb{R}$) and so it suffices to show that there is precisely one solution of $J(\tau) = c$ in F°. The idea is to express

the number of solutions of the equation $J(\tau) = c$ as the number of residues of an appropriate function, so that we may use Cauchy's Residue Theorem (a similar strategy was employed earlier in the proof of Theorem 2.12). By Theorem 3.18 and Corollary 3.22, we know that J is analytic and not identically equal to c, and so the function

$$g(\tau) = \frac{J'(\tau)}{J(\tau) - c}$$

is meromorphic on $\mathbb{H}$. By an argument similar to that of Theorem 2.12, a point $a \in \mathbb{H}$ is a solution of $J(\tau) = c$ with multiplicity k if and only if $g(\tau)$ has a pole with residue k at a. Using the Laurent series expansion of J, we may express $g(\tau)$ as a function of $q = e^{2\pi i \tau}$, which has a pole at $q = 0$ since $J(\tau)$ does. Thus, $g(\tau)$ is analytic for all sufficiently small non-zero $|q|$; that is, provided that $\mathrm{Im}(\tau)$ is sufficiently large, say, $\mathrm{Im}(\tau) \geq K$ for some $K > 1$. Hence the poles of $g(\tau)$ in F all lie within the interior of the set $G = \{\tau \in F : \mathrm{Im}(\tau) \leq K\}$, as depicted below.



By the Residue Theorem, the sum of the residues of $g(\tau)$ in G (and thus the number of solutions of $J(\tau) = c$, counting multiplicities), is given by

$$\frac{1}{2\pi i} \int_{\partial G} g(\tau) d\tau, \tag{3.25}$$

where the boundary ∂G is given the counterclockwise (positive) orientation. Since the sides $\mathrm{Re}(\tau) = -1/2$ and $\mathrm{Re}(\tau) = 1/2$ are equivalent under the transformation $\tau \mapsto \tau + 1$ of Γ, $J(\tau)$, and hence $g(\tau)$, take the same values at equivalent points on these sides. Since the sides have opposite orientation, the integrals of $g(\tau)$ along these two sides cancel. Similarly, using the transformation $\tau \mapsto -1/\tau$ of Γ, we see that the integral from ρ to i cancels with the integral from i to $\rho + 1$. We conclude that evaluating the integral of $g(\tau)$ along ∂G amounts to evaluating it over the horizontal line γ connecting the points $1/2 + iK$ and $-1/2 + iK$. That is,

$$\int_{\partial G} g(\tau) d\tau = \int_{\gamma} g(\tau) d\tau.$$

To calculate this integral, we notice that away from the poles of $g(\tau)$, each branch of the logarithm satisfies

$$\frac{d}{d\tau}(\log(J(\tau) - c)) = \frac{J'(\tau)}{J(\tau) - c} = g(\tau),$$

and so

$$\int_\gamma g(\tau)d\tau = \log(J(\tau)-c)\big|_\gamma,$$

where the change in the value of $\log(J(\tau)-c)$ arises from analytic continuation along γ. Indeed, as τ follows γ, the point q winds once (in the clockwise, negative direction) around the circle C given by $|q| = e^{-2\pi k}$, beginning and finishing at $-e^{-2\pi K}$. By Theorem 3.19, $q(J(\tau)-c)$ is analytic and non-zero for all $0 \leq |q| \leq e^{-2\pi K}$. Since this set is simply connected, the monodromy theorem implies that

$$\log(q(J(\tau)-c))\big|_\gamma = 0,$$

and therefore

$$\log(J(\tau)-c)\big|_\gamma = \big[\log(q(J(\tau)-c)) - \log q\big]_\gamma = [-\log(q)]_\gamma = 2\pi i.$$

By (3.25), we have that the number of solutions of $J(\tau) = c$ in F is equal to 1, as required.

Finally suppose that $c \in \mathbb{R}$. By Theorem 3.23, there is at least one orbit of Γ on which J takes the value c. If there were two such orbits, then there would exist two non-equivalent solutions τ_1 and τ_2 of the equation $J(\tau) = c$. By choosing $c' \in \mathbb{C}\setminus\mathbb{R}$ sufficiently close to c, we would obtain two non-equivalent solutions to the equation $J(\tau) = c'$. But we have already shown that this is impossible; hence τ_1 and τ_2 must be in the same orbit of Γ, and thus the orbit is unique. □

We are finally able to prove the converse to Theorem 2.25.

Theorem 3.26. *If $c_2, c_3 \in \mathbb{C}$ satisfy $c_2^3 - 27c_3^2 \neq 0$, then there is a lattice $\Omega \subset \mathbb{C}$ with $g_k(\Omega) = c_k$, for $k = 2, 3$. That is, if $p(z) = 4z^3 - c_2 z - c_3$, where c_2 and c_3 are as above, then the elliptic curve $y^2 = p(z)$ is homeomorphic to $\mathbb{C}/\Omega$ for some lattice Ω.*

Proof. There are three separate cases to consider. Suppose first that $c_2 = 0$. Then by hypothesis, $c_3 \neq 0$. By Corollary 3.22, we know that $g_2(\rho) = 0$, and since $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$ never vanishes on $\mathbb{H}$, we conclude that $g_3(\rho) \neq 0$. Thus there exists some $\mu \in \mathbb{C}\setminus\{0\}$ such that $\mu^{-6}g_3(\rho) = c_3$. So, if we set

$$\Omega = \mu\Omega(1,\rho) = \Omega(\mu, \mu\rho),$$

then we have $g_2(\Omega) = \mu^{-4}g_2(\rho) = 0 = c_2$, and $g_3(\Omega) = \mu^{-6}g_3(\rho) = c_3$, as required.

Suppose now that $c_3 = 0$, so that $c_2 \neq 0$. By Corollary 3.22, $g_3(i) = 0$, and so similarly to as before, we must have $g_2(i) \neq 0$. Hence, there exists $\mu \in \mathbb{C}\setminus\{0\}$ such that $\mu^{-4}g_2(i) = c_2$. Setting

$$\Omega = \mu\Omega(1,i) = \Omega(\mu, \mu i),$$

we find that $g_2(\Omega) = \mu^{-4}g_2(i) = c_2$, and $g_3(\Omega) = \mu^{-6}g_3(i) = 0 = c_3$, as desired.

We now consider the general case when $c_2, c_3 \neq 0$. By Theorem 3.24, there exists some $\tau \in \mathbb{H}$ such that

$$\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} = J(\tau) = \frac{c_2^3}{c_2^3 - 27c_3^2}.$$

As $c_2 \neq 0$, we have $g_2(\tau) \neq 0$. We also see that $g_3(\tau) \neq 0$, since if $g_3(\tau) = 0$, then $J(\tau) = 1$, and hence $c_3 = 0$, a contradiction. Thus after some algebraic

manipulations, we obtain the well-defined equality of non-zero complex numbers

$$\frac{c_2^3}{g_2(\tau)^3} = \frac{c_3^2}{g_3(\tau)^2}. \tag{3.27}$$

There exists some $\mu \in \mathbb{C} \setminus \{0\}$ such that $\mu^{-4} = c_2/g_2(\tau)$. By (3.27), we obtain

$$\mu^{-12} = \frac{c_2^3}{g_2(\tau)^3} = \frac{c_3^2}{g_3(\tau)^2}, \text{ and so,}$$
$$\mu^{-6} = \pm\frac{c_3}{g_3(\tau)}.$$

Replacing μ by $i\mu$ if necessary, we have $\mu^{-4} = c_2/g_2(\tau)$ and $\mu^{-6} = c_3/g_3(\tau)$. Thus

$$\Omega = \mu\Omega(1, \tau) = \Omega(\mu, \mu\tau)$$

is our desired lattice. The second statement of the theorem is immediate from Theorem 2.25. □

As a final remark, we note that it is actually possible to prove a stronger result. Namely, if $p(z)$ is a polynomial with distinct roots (so that is can be put in the Weierstrass normal form $4z^3 - c_2z - c_3$, with $c_2^3 - 27c_3^2 \neq 0$), then the Riemann surface of $w = \sqrt{p(z)}$ is in fact conformally equivalent to $\mathbb{C}/\Omega$ for some lattice $\Omega \subset \mathbb{C}$ (see Theorem 6.5.11 of [1]). As we remarked below Definition 3.1, two tori $\mathbb{C}/\Omega$ and $\mathbb{C}/\Omega'$ are conformally equivalent if and only if they are similar. By Theorem 3.4, this occurs if and only if their moduli τ and τ' are in the same orbit of Γ on $\mathbb{H}$. Thus the points of the quotient space $\mathbb{H}/\Gamma$ represent the set of all complex structures that may be placed on an elliptic curve, yielding yet another beautiful result concerning elliptic curves over $\mathbb{C}$.

Acknowledgments

I would like to thank Professor Matthew Emerton for meeting with me many times throughout the summer to teach me about elliptic curves; my knowledge of the subject was greatly enriched by having the opportunity to learn from him. I would also like to thank Thomas Hameister for the many helpful discussions we had about elliptic curves and algebraic geometry, and for his reading this paper and providing me with very useful feedback. Additionally, I thank Yuchen Chen and Ethan Schondorf for the several discussions we had about this subject. Last but certainly not least, I would like to thank Professor Peter May for the effort he puts into organizing the UChicago REU, and for giving me the opportunity to participate in it.

References

[1] Jones, G.A. and Singerman, D *Complex Functions: An algebraic and geometric viewpoint* Cambridge University Press, Cambridge, 1987.
[2] Shafarevich, I. *Basic Algebraic Geometry I: Varieties in Projective Space* Springer-Verlag, 2013.
[3] Silverman, Joseph H. *The Arithmetic of Elliptic Curves* Springer, 2009.
[4] Reid, Miles. *Undergraduate Algebraic Geometry* Cambridge University Press, 1988.
[5] Shurman, Jerry. *Complex Tori as Elliptic Curves* *https : //people.reed.edu/ jerry/*311*/toriec.pdf*

[6] Fraser, Jonathan M. *MT 5830: Topics in Geometry and Analysis* $http://www.mcs.st-andrews.ac.uk/\ jmf32/teaching.html$ 2017.